Notice of Allowability	Application No.	Applicant(s)	
	10/038,147	GREENBERG ET AL.	
	Examiner	Art Unit	
	Aubrey H. Berger	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *application filed on 03 January 2002*.

2. ☒ The allowed claim(s) is/are *1-4*.

3. ☒ The drawings filed on *05 March 2002* are accepted by the Examiner.

4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

6. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

7. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

EXAMINER'S AMENDMENT

1. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with William Meise on August 11, 2005.

The application has been amended as follows:

a. In claim 1, lines 6-7, "the various parties" has been replaced with "at least said first and second users".

b. In claim 1, line 11, "the first salt from said plurality of salts" has been replaced with "a first hash salt from said plurality of hash salts".

c. In claim 1, lines 14-15, "the second of said plurality of hash salts" has been replaced with "a second of said plurality of hash salts".

d. In claim 1, lines 18-19, "the third of said plurality of hash salts" has been replaced with "a third of said plurality of hash salts".

e. In claim 1, lines 22-23, "the forth of said plurality of hash salts" has been replaced with "a forth of said plurality of hash salts."

f. In claim 1, line 39, "using as a key using said at least" has been replaced with "using as a key, said at least".

g. In claim 1, line 47, "said forth salt" has been replaced with "said forth hash salt".

h. In claim 2, line 2, the word "of" has been removed.

i. In claim 2, lines 5-6, "the first salt from said plurality of salts" has been replaced with "a first hash salt from said plurality of hash salts."

j. In claim 3, lines 6-7, "the various parties" has been replaced with "at least said first and second users".

k. In claim 3, line 11, "the first salt from said plurality of salts" has been replaced with "a first hash salt from said plurality of hash salts".

l. In claim 3, line 14-15, "the second of said plurality of hash salts" has been replaced with "a second of said plurality of hash salts".

m. In claim 3, lines 18-19, "the third of said plurality of hash salts" has been replaced with "a third of said plurality of hash salts".

n. In claim 3, lines 22-23, "the forth of said plurality of hash salts" has been replaced with "a forth of said plurality of hash salts."

o. In claim 3, line 52, "using as a key using one of" has been replaced with "using as a key, one of"

p. In claim 3, line 60, "said forth salt" has been replaced with "said forth hash salt".

Allowable Subject Matter

2. Claims 1-4 are allowed.

3. The following is an examiner's statement of reasons for allowance: U.S. Patent 6,584,564 to Olkin et al. (Olkin) discloses a method for communication among at least a first/sender and second users/receiver (Fig. 1, #12 and #16), communicating by means of a communication system, said method comprising

the steps of: providing a first unique identifier/password, from said first user/sender to said second user/receiver. Olkin further discloses a unique identifier/password, wherein a hash salt is used to modify the unique identifier/password, to produce a hash. The hash is stored in place of the unique identifier/password, while the unique identifier/password, is discarded (col. 11, lines 49-54). Further, U.S. Patent 6,064,736 to Davis et al. (Davis) teaches a method for generating a second salt and rehashing the unique identifier/password first hash and second salt to produce a second hash (Figure 5). Davis also teaches comparing data hashes to validate their authenticity (col. 2, lines 9-11). Further, European Patent 0849713 to Blank teaches unique identifier/PIN code is transformed following a predetermined deterministic transformation and then encrypting the unique identifier/PIN code. Further U.S. Patent 5,937,066 to Gennaro et al. (Gennaro) teaches entering into an agreement between the various parties as to a plurality of hash salts (col. 22, lines 28-31). However, regarding claims 1-2, the prior art relied upon fails to teach or suggest the combination of limitations that comprise of the steps of performing a hash operation on at least a portion of said first data hash using a third of said plurality of hash salts; performing a hash operation on at least a portion of said third data hash using a forth of said plurality of hash salts; discarding third data hash, performing a hash operation using a further hash salt on at least a portion of said first unique identifier and data deterministically derived from said unique identifier to produce a fifth data hash, encrypting a random number with a key which includes at least a deterministic transformation

of said second data hash; decrypting said encrypted random number using as a key said at least a deterministic transformation of said second data hash; transmitting extracted random number and said third data hash; performing a hash operation on said third data hash by the use of said forth salt to generate a sixth data hash; comparing said forth and sixth data hashes, deeming said message to be from said first user; discarding said third data hash; further comprising after said steps, performing a hash operation on said first unique identifier and a deterministic transformation of said first unique identifier, using the first salt to produce a fist data hash and performing a hash operation using a further has salt to produce a fifth data hash; and discarding said first unique identifier. Furthermore, regarding claims 3-4, the prior art relied upon fails to teach or suggest the combination of limitations that comprise of the steps of storing said second and forth data hashes in memory at locations established by said fifth data hash; performing a hash operation on at least a portion of one of said first unique identifier and data deterministically derived from said unique identifier, using said fifth data hash to produce a replica of said fifth data hash; accessing memory at locations established by said replica to obtain second an forth data hashes; further comprising discarding said fifth data hash.

4. Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Aubrey H. Berger whose telephone number is (571)272-8155. The examiner can normally be reached on Monday - Thursday, 7:30 a.m. - 5:00 p.m..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Greg Morse can be reached on (571)272-3838. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

AHB

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100